

(11)特許出願公開番号
特開2000-113586
(P2000-113586A)

(43)公開日 平成12年4月21日(2000.4.21)

(51) Int.Cl.⁷
G 1 1 B 20/10
H 0 4 L 9/10
9/32

識別記号

F I
G 1 1 B 20/10
H 0 4 L 9/00

テ-マコート* (参考)

H 5D044

621A 5J104

6 7 3 E

6 7 3 C

審査請求 未請求 請求項の数4 OL (全 11 頁)

(21)出願番号 特願平10-280236

(22)出願日 平成10年10月1日(1998.10.1)

(71)出願人 000004329

日本ビクター株式会社

神奈川県横浜市神奈川区守屋町3丁目12番地

(72)発明者 平田 渥美

神奈川県横浜市神奈川区守屋町3丁目12番地 日本ビクター株式会社内

(74) 代理人 100083806

井理士 三好 秀和 (外9名)

Fターム(参考) 5D044 AB05 AB07 CC04 DE49 GK17

5J104 AA13 AA16 EA17 NA02 NA30

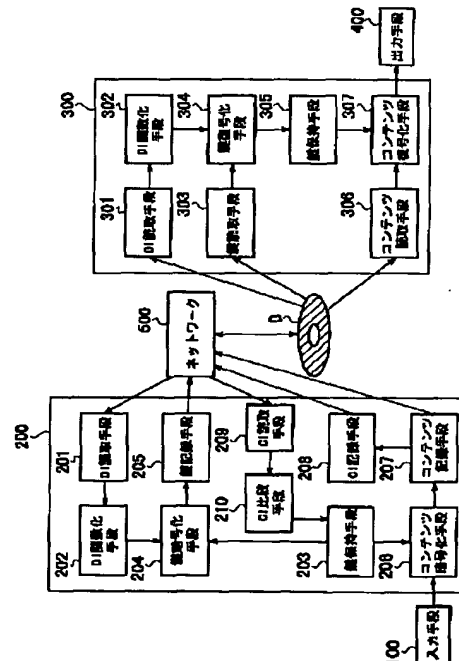
PA14

(54) 【発明の名称】 情報保護方法及び情報を保護するための情報記録媒体

(57) 【要約】

【課題】 情報を放送や通信手段を介して伝達し記録型ディスクに記録する際に、不正コピーを防止するとともに、正当に権利を得た者に対しては容易にコピーを許可することのできる情報保護方法を提供することにある。

【解決手段】 本発明の情報保護方法は、入力されたコンテンツを鍵によって暗号化して情報記録媒体Dに記録し、鍵によって復号化して再生する情報保護方法であって、各情報記録媒体に特有の固有情報と各コンテンツに特有の識別情報とを情報記録媒体Dに記録し、C1比較手段210において識別情報からコンテンツを暗号化した鍵を見つけることによってコンテンツを復号化して再生することを特徴とする。



【特許請求の範囲】

【請求項 1】 それぞれ特有の固有情報を有する情報記録媒体に鍵によって情報を暗号化して記録し、前記情報記録媒体に記録された情報を前記鍵によって復号化して再生する情報保護方法であって、前記固有情報によって暗号化された前記鍵と各情報にそれぞれ特有の識別情報とを前記情報記録媒体に記録し、前記情報を暗号化した前記鍵を前記識別情報によって特定し、前記暗号化された情報を復号化して再生することを特徴とする情報保護方法。

【請求項 2】 それぞれ特有の固有情報を有する情報記録媒体に情報を暗号化して記録し、前記情報記録媒体に記録された情報を復号化して再生する情報保護方法であって、前記固有情報によって暗号化された情報と関数化された前記固有情報とを前記情報記録媒体に記録し、前記関数化された固有情報を復号して得た固有情報から差分を生成することによって前記暗号化された情報を復号化して再生することを特徴とする情報保護方法。

【請求項 3】 各情報記録媒体毎にそれぞれ特有の固有情報が改変できない方法で、あるいは改変できないエリアに記録され、さらに各情報毎にそれぞれ特有の識別情報が記録されていることを特徴とする情報を保護するための情報記録媒体。

【請求項 4】 各情報記録媒体毎にそれぞれ特有の固有情報が改変できない方法で、あるいは改変できないエリアに記録され、さらに前記固有情報から生成された差分が記録されていることを特徴とする情報を保護するための情報記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、記録型ディスクに記録された情報を保護するための情報保護方法に関し、特に個々のディスクに特有の固有情報と個々のコンテンツに特有の識別情報とをディスクに記録することによって、不正コピーを防止するとともに、権利者に対しては容易にコピーを許可することのできる情報保護方法及び情報を保護するための情報記録媒体に関する。

【0002】

【従来の技術】 CD-R、PD、DVD-RAM、DVD-RWなどの記録型ディスク媒体（以下ディスクという）及び装置において、ネットワークあるいは放送を介して伝送され、正当に権利を得て 1 回記録することを許された場合、映画などの動画像、静止画像、音楽などのコンテンツは簡単に記録することができなければならない。また、記録後のディスクは、正規の装置であればどの装置を利用して再生できるようにしたいという要求がある。

【0003】 一方、そのような記録型ディスク媒体及び装置において、不正にコピーされることを防止して著作

権を守る必要があるが、正当な権利で容易に記録・再生できることとコピーを防止することは背反しており両立させることが困難であった。

【0004】 そこで、このような矛盾を解決すべく従来の情報保護装置では、固有情報 DI を利用することによって不正なコピーを防止していた。

【0005】 図 4 に示すように、従来の情報保護装置は、動画像、静止画像、音楽などのコンテンツを入力する入力手段 10 と、一般的な情報記録媒体 D にコンテンツなどの情報を暗号化して記録する情報記録手段 20 と、情報記録媒体 D に記録された情報を復号化して再生する情報再生手段 30 と、復号化されたコンテンツなどの情報を出力する出力手段 40 とを含んでいる。

【0006】 ここで、情報記録手段 20 は、情報記録媒体 D 毎にそれぞれ記録された固有情報 DI を読み取る DI 読み取り手段 21 と、この DI 読み取り手段 21 によって読み取られた固有情報 DI を関数化あるいは暗号化（以下、関数化という）する DI 関数化手段 22 と、この DI 関数化手段 22 によって関数化された固有情報 F(DI) によって入力手段 10 から入力されたコンテンツ CT を暗号化するコンテンツ暗号化手段 23 と、このコンテンツ暗号化手段 23 によって暗号化されたコンテンツ E(CT) を情報記録媒体 D に記録するコンテンツ記録手段 24 とから構成されている。

【0007】 また情報再生手段 30 は、情報記録媒体 D 毎にそれぞれ記録された固有情報 DI を読み取る DI 読み取り手段 31 と、この DI 読み取り手段 31 によって読み取られた固有情報 DI を関数化する DI 関数化手段 32 と、情報記録媒体 D に記録された暗号化されたコンテンツ E(CT) を読み取るコンテンツ読み取り手段 33 と、このコンテンツ読み取り手段 33 によって読み取られた暗号化されたコンテンツ E(CT) を関数化された固有情報 F(DI) によって復号化して出力手段 40 へ出力するコンテンツ復号化手段 34 とから構成されている。

【0008】 次に、この従来の情報保護装置の動作について説明する。

【0009】 まず、コンテンツ CT が入力手段 10 より入力されると、ディスク D の固有情報 DI を DI 読み取り手段 21 が読み取り、この固有情報 DI を DI 関数化手段 22 で関数化して F(DI) とする。そして、コンテンツ暗号化手段 23 において、入力されたコンテンツ CT を関数化された固有情報 F(DI) で暗号化して E(CT) とし、コンテンツ記録手段 24 によってディスク D に記録する。

【0010】 そして、ユーザーは情報再生手段 30 においてディスク D を再生する場合には、まずディスク D から DI 読み取り手段 31 によってディスク D の固有情報 DI を読み取り、この固有情報 DI を DI 関数化手段 32 で関数化して F(DI) とする。そして、次に暗号化されたコンテンツ E(CT) をコンテンツ読み取り手段 33

によってディスクDから読み取り、コンテンツ復号化手段34において関数化された固有情報F(DI)によって復号化してコンテンツCTとし、出力手段40に送り、出力することになる。

【0011】また、図5に示す従来の情報保護装置では、図4の装置と同様に入力手段10と、情報記録手段20と、情報再生手段30と、出力手段40とを含んでいる。

【0012】ここで、情報記録手段20は、図4に示す装置の構成要素の他に、入力されるコンテンツCTを暗号化するための鍵KEYを保持する鍵保持手段25と、この鍵保持手段25により保持された鍵KEYを関数化された固有情報F(DI)によって暗号化する鍵暗号化手段26と、この鍵暗号化手段26によって暗号化された鍵E(KEY)を情報記録媒体Dに記録する鍵記録手段27とをさらに含んでいる。

【0013】また情報再生手段30は、図4に示す装置の構成要素の他に、情報記録媒体Dに記録された暗号化された鍵E(KEY)を読み取る鍵読み取り手段35と、暗号化された鍵E(KEY)を関数化された固有情報F(DI)によって復号化する鍵復号化手段36と、この鍵復号化手段36によって復号化された鍵KEYを保持する鍵保持手段37とをさらに含んでいる。

【0014】次に、この従来の情報保護装置の動作について説明する。

【0015】まず、コンテンツCTが入力手段10より入力されると、コンテンツ暗号化手段23において、入力されたコンテンツCTを鍵保持手段25に保持された鍵KEYによって暗号化してE(CT)とし、コンテンツ記録手段24によってディスクDに記録する。一方、DI読み取り手段21ではディスクDの固有情報DIを読み取り、この固有情報DIをDI関数化手段22で関数化してF(DI)とする。そして、鍵暗号化手段26において、鍵保持手段25で保持された鍵KEYを暗号化してE(KEY)とし、鍵記録手段27によってディスクDに記録する。

【0016】そして、ユーザーは情報再生手段30においてディスクDを再生する場合には、まずディスクDからDI読み取り手段31によってディスクDの固有情報DIを読み取り、この固有情報DIをDI関数化手段32で関数化してF(DI)とする。そして、鍵読み取り手段35によって読み取られた暗号化された鍵E(KEY)を、鍵復号化手段36において関数化された固有情報F(DI)で復号化して鍵KEYとし、鍵保持手段37に保持する。

【0017】一方、暗号化されたコンテンツE(CT)はコンテンツ読み取り手段33によってディスクDから読み取られ、コンテンツ復号化手段34において鍵保持手段37に保持された鍵KEYによって復号化してコンテンツCTとし、出力手段40に送られ出力されることに

なる。

【0018】また、図4と図5に示す従来の情報保護装置において、ネットワーク（放送型、ポイント・ツー・ポイント型、バスラインなど任意の形態を含む）を介してコンテンツを伝送する場合について、図6、図7にそれぞれ示す。基本的な構成は図4、図5と同じでディスクDに記録する際にネットワーク50が介在する。

【0019】

【発明が解決しようとする課題】このように、上述した従来の情報保護装置では、確かに不正なコピーは防止できるものの、コンテンツを供給する側としては、不正なコピーを防止するということと同時に、正規の手続きをした者に対してはコピーを許し、それによって料金収入を得たいという要求があった。

【0020】しかしながら、従来の情報保護装置では、たとえ正規に権利を得た者であっても、コピーされたディスクを再生することはできなかった。

【0021】本発明は上記事情に鑑みてなされたものであり、その目的は、個々のディスクに特有の固有情報と個々のコンテンツに特有の識別情報とを情報記録媒体に記録することによって、不正コピーを防止するとともに、正当に権利を得た者に対しては容易にコピーを許可することのできる情報保護方法を提供することにある。

【0022】

【課題を解決するための手段】上記目的を達成するために、第1の発明である情報保護方法は、それぞれ特有の固有情報を有する情報記録媒体に鍵によって情報を暗号化して記録し、前記情報記録媒体に記録された情報を前記鍵によって復号化して再生する情報保護方法であって、前記固有情報によって暗号化された前記鍵と各情報にそれぞれ特有の識別情報とを前記情報記録媒体に記録し、前記情報を暗号化した前記鍵を前記識別情報によって特定し、前記暗号化された情報を復号化して再生することを特徴とする。

【0023】この第1の発明によれば、各情報記録媒体に特有の固有情報だけでなく、各情報に特有の識別情報とを利用することによって、不正コピーを防止できるとともに正規の手続きをした者は容易に情報記録媒体のコピーができるようになった。

【0024】第2の発明である情報保護方法は、それぞれ特有の固有情報を有する情報記録媒体に情報を暗号化して記録し、前記情報記録媒体に記録された情報を復号化して再生する情報保護方法であって、前記固有情報によって暗号化された情報と関数化された前記固有情報とを前記情報記録媒体に記録し、前記関数化された固有情報を復号して得た固有情報から差分を生成することによって前記暗号化された情報を復号化して再生することを特徴とする。

【0025】この第2の発明によれば、関数化された固有情報を復号化した得た固有情報から差分を生成し、こ

の差分を利用して暗号化された情報を復号化することによって、不正コピーを防止できるとともに正規の手続きをした者は容易に情報記録媒体のコピーができるようになった。

【0026】第3の発明である情報を保護するための情報記録媒体は、各情報記録媒体毎にそれぞれ特有の固有情報が改変できない方法で、あるいは改変できないエリアに記録され、さらに各情報毎にそれぞれ特有の識別情報が記録されていることを特徴とする。

【0027】この第3の発明によれば、各情報記録媒体に特有の固有情報だけでなく、各情報に特有の識別情報とを利用することによって、不正コピーを防止できるとともに正規の手続きをした者は容易に情報記録媒体のコピーができるようになった。

【0028】第4の発明である情報を保護するための情報記録媒体は、各情報記録媒体毎にそれぞれ特有の固有情報が改変できない方法で、あるいは改変できないエリアに記録され、さらに前記固有情報から生成された差分が記録されていることを特徴とする。

【0029】この第4の発明によれば、関数化された固有情報を復号化した得た固有情報から差分を生成し、この差分を利用して暗号化された情報を復号化することによって、不正コピーを防止できるとともに正規の手続きをした者は容易に情報記録媒体のコピーができるようになった。

【0030】

【発明の実施の形態】以下、本発明に係る情報保護方法の第1の実施形態を図面に基づいて説明する。本実施形態の情報保護方法を実現する装置は、各情報記録媒体にそれぞれ特有の固有情報と各コンテンツに特有の識別情報とを利用することによって、コンテンツを暗号化するものである。

【0031】図1は本実施形態の情報保護装置の構成を示すブロック図である。図1に示すように、本実施形態の情報保護装置は、動画像、静止画像、音楽などのコンテンツを入力する入力手段100と、一般的な情報記録媒体Dにコンテンツなどの情報を暗号化して記録する情報記録手段200と、情報記録媒体に記録された情報を復号化して再生する情報再生手段300と、復号化されたコンテンツなどの情報を出力する出力手段400とを含んでいる。

【0032】ここで、情報記録手段200は、情報記録媒体D毎にそれぞれ記録された固有情報DIを読み取るDI読み取り手段201と、このDI読み取り手段201によって読み取られた固有情報DIを関数化するDI関数化手段202と、入力されるコンテンツCTを暗号化するための鍵KEYを保持する鍵保持手段203と、この鍵保持手段203により保持された鍵KEYを関数化された固有情報F(DI)によって暗号化する鍵暗号化手段204と、この鍵暗号化手段204によって暗号化

された鍵E(KEY)をネットワーク500を介して情報記録媒体Dに記録する鍵記録手段205と、鍵保持手段203により保持された鍵KEYによって入力手段100から入力されたコンテンツCTを暗号化するコンテンツ暗号化手段206と、このコンテンツ暗号化手段206によって暗号化されたコンテンツE(CT)をネットワーク500を介して情報記録媒体Dに記録するコンテンツ記録手段207と、このコンテンツ記録手段207によって記録された暗号化されたコンテンツE(CT)に特有の識別情報CIをネットワーク500を介して情報記録媒体Dに記録するCI記録手段208と、情報記録媒体Dに記録されている識別情報CIを読み取るCI読み取り手段209と、コンテンツとそのコンテンツを暗号化した鍵との対応について記録したコンテンツリストを有し、このコンテンツリストと識別情報CIとを比較し、コンテンツに対応する鍵を見つけるCI比較手段210とから構成されている。

【0033】また情報再生手段300は、情報記録媒体D毎にそれぞれ記録された固有情報DIを読み取るDI読み取り手段301と、このDI読み取り手段301によって読み取られた固有情報DIを関数化するDI関数化手段302と、情報記録媒体Dに記録された暗号化された鍵E(KEY)を読み取る鍵読み取り手段303と、暗号化された鍵E(KEY)を関数化された固有情報F(DI)によって復号化する鍵復号化手段304と、この鍵復号化手段304によって復号化された鍵KEYを保持する鍵保持手段305と、コンテンツ記録手段207によって情報記録媒体Dに記録された暗号化されたコンテンツE(CT)を読み取るコンテンツ読み取り手段306と、暗号化されたコンテンツE(CT)を鍵保持手段305に保持された鍵KEYによって復号化して出力手段400へ出力するコンテンツ復号化手段307とから構成されている。

【0034】次に、本実施形態の情報保護装置の動作について説明する。

【0035】まず、コンテンツCTが入力手段100より入力されると、コンテンツ暗号化手段206において、入力されたコンテンツCTを鍵保持手段203に保持された鍵KEYによって暗号化してE(CT)とし、コンテンツ記録手段207によってネットワーク500を介してディスクDに記録する。そして、この暗号化されたコンテンツE(CT)に特有の識別情報CIもCI記録手段208によって記録する。

【0036】一方、DI読み取り手段201ではディスクDの固有情報DIをネットワーク500を介して読み取り、この固有情報DIをDI関数化手段202で関数化してF(DI)とする。そして、鍵暗号化手段204において、鍵保持手段203で保持されている鍵KEYを暗号化してED(KEY)とし、鍵記録手段205によってネットワーク500を介してディスクDに記録する。

【0037】次に、ユーザーが情報再生手段300において情報記録媒体Dを再生する場合について説明する。まず、情報記録手段200で正規に記録されたオリジナルのディスクDを再生する場合には、まずディスクDからDI読み取り手段301によってディスクDの固有情報DIを読み取り、この固有情報DIをDI関数化手段302で関数化してF(DI)とし、鍵読み取り手段303によって読み取られた暗号化された鍵ED_I(KEY)を、鍵復号化手段304において関数化された固有情報F(DI)で復号化して鍵KEYとし、鍵保持手段305に保持する。そして、コンテンツ読み取り手段306

で、暗号化されたコンテンツE(CT)をディスクDから読み取り、コンテンツ復号化手段307において鍵保持手段305に保持されている鍵KEYによって復号化してコンテンツCTとし、出力手段400に送られ出力されることになる。

【0038】次に、コピーされたディスクD'を再生する場合について説明する。この場合にはDI読み取り手段301によって読み取られた固有情報DI'がオリジナルディスクDの固有情報DIと異なるので、このままではディスクD'を再生することができない。そこで、情報記録手段200のDI読み取り手段201によって固有情報DI'を読み取り、この固有情報DI'をDI関数化手段202で関数化してF(DI')とする。

【0039】また、CI読み取り手段209ではネットワーク500を介してディスクDに記録されている識別情報CIを読み取り、CI比較手段210において、この識別情報CIとコンテンツリストとを比較し、対応するコンテンツの鍵KEYを見つけ、鍵保持手段203で保持する。そして、鍵暗号化手段204においてこの鍵KEYをDI関数化手段202で関数化されたF(DI')によって暗号化し、ED_I(KEY)として鍵記録手段205でネットワーク500を介してディスクD'に記録する。この際、ディスクD'にはオリジナルのディスクDの固有情報DIで暗号化された鍵ED_I(KEY)が記録されているが、その上に新たに暗号化された鍵ED_I(KEY)を重ね書きするか、あるいは別の領域に追記してもよい。ただし、追記する場合には再生時に最新の鍵についての情報を確認してから再生することになる。また、この新たに暗号化された鍵ED_I(KEY)をディスクD'に記録する際にコンテンツを供給する側では料金を徴収すればよい。

【0040】そして、情報再生手段300では、DI読み取り手段301によってディスクD'の固有情報DI'を読み取り、DI関数化手段302で関数化してF(DI')とする。そして、鍵読み取り手段303によって、新しく暗号化された鍵ED_I(KEY)を、鍵復号化手段304において関数化された固有情報F(DI')で復号化して鍵KEYとして鍵保持手段305に保持する。新たな暗号化された鍵ED_I(KEY)はF(DI')

によって暗号化されているので、オリジナルディスクDの固有情報DIではなく、コピーディスクD'の固有情報DI'で復号化することができる。

【0041】そして、コンテンツ読み取り手段306では暗号化されたコンテンツE(CT)をディスクD'から読み取り、コンテンツ復号化手段307において鍵保持手段305に保持されている鍵KEYによって復号化してコンテンツCTとし、出力手段400に送られ出力されることになる。

【0042】尚、本実施形態ではDI関数化手段202によって固有情報DIを関数化し、この関数化された固有情報F(DI)によってコンテンツCTを暗号化しているが、固有情報DIを関数化せずに直接固有情報DIによってコンテンツCTを暗号化することもできる。この場合には情報再生手段300においても固有情報DIを関数化することなく、固有情報DIによってコンテンツCTを復号化する。

【0043】また、本実施形態では、ネットワーク500を介して情報記録媒体Dへの記録、読み取りを実行しているが、ネットワーク500を介せずに情報記録手段200から情報記録媒体Dに直接記録等してもよい。

【0044】このように、第1の実施形態の情報保護装置では、識別情報CIからコンテンツを暗号化した鍵を、コンテンツリストと比較することによって見つけ出し、その鍵をコピーディスクD'の固有情報DI'によって暗号化するので、情報再生手段300ではコピーディスクD'の固有情報DI'から鍵を復号化することができ、従ってコピーディスクD'を再生することができる。

【0045】また、コンテンツを供給する側としては、新たに暗号化された鍵ED_I(KEY)をディスクD'に記録する際に、料金を徴収すればよいので、利益を確保することができるとともに、ディスクコピーによってコンテンツの使用を許可できるのでコンテンツの流通性をよくすることができる。

【0046】次に、第2の実施形態の情報保護方法について説明する。

【0047】図2は第2の実施形態の情報保護方法を実現する装置の構成を示すブロック図である。図2に示すように、本実施形態の情報保護装置は、第1の実施形態の情報保護装置と同様に、入力手段100と、情報記録手段200と、情報再生手段300と、出力手段400とを含んでおり、情報記録手段200は、情報記録媒体D毎にそれぞれ記録された固有情報DIをネットワーク500を介して読み取る第1DI読み取り手段251と、この第1DI読み取り手段251によって読み取られた固有情報DIを関数化する第1関数化手段252と、この第1関数化手段252で関数化された固有情報F(DI)によって、入力手段100から入力されたコンテンツCTを暗号化するコンテンツ暗号化手段253

と、このコンテンツ暗号化手段253によって暗号化されたコンテンツE(CT)をネットワーク500を介して情報記録媒体Dに記録するコンテンツ記録手段254と、第1DI読み取り手段251によって読み取られた固有情報DIを第1関数化手段252と異なる関数で関数化する第2関数化手段255と、この第2関数化手段255によって関数化された固有情報F'(DI)をネットワーク500を介して情報記録媒体Dに記録するDI記録手段256と、情報記録媒体Dに記録されている関数化された固有情報F'(DI)をネットワーク500を介して読み取る第2DI読み取り手段257と、この関数化された固有情報F'(DI)を、第2関数化手段255で関数化したときの逆関数 F'^{-1} (暗号の復号化を含む)によって復号化するDI復号化手段258と、第1関数化手段252で関数化された固有情報F(DI)、F(DI')の差分 $F(DI)-F(DI')$ を生成する差分手段259と、この差分手段259によって生成された差分 $F(DI)-F(DI')$ をネットワーク500を介して情報記録媒体Dに記録する差分記録手段260とから構成されている。

【0048】また情報再生手段300は、情報記録媒体D毎にそれぞれ記録された固有情報DIを読み取るDI読み取り手段301と、このDI読み取り手段301によって読み取られた固有情報DIを関数化するDI関数化手段302と、情報記録媒体Dに記録された差分 $F(DI)-F(DI')$ を読み取る差分読み取り手段308と、この差分 $F(DI)-F(DI')$ と関数化された固有情報F(DI')とを合成して関数化された固有情報F(DI)を生成する合成手段309と、情報記録媒体Dに記録された暗号化されたコンテンツE(CT)を読み取るコンテンツ読み取り手段306と、このコンテンツ読み取り手段306によって読み取られた暗号化されたコンテンツE(CT)を、合成手段309によって生成された関数化された固有情報F(DI)によって復号化して出力手段400へ出力するコンテンツ復号化手段307とから構成されている。

【0049】次に、第2の実施形態の情報保護装置の動作について説明する。

【0050】まず、コンテンツCTが入力手段100より入力されると、ディスクDの固有情報DIを第1DI読み取り手段251が読み取り、この固有情報DIを第1関数化手段252で関数化してF(DI)とする。そして、コンテンツ暗号化手段253において、入力されたコンテンツCTを関数化された固有情報F(DI)で暗号化してE(CT)とし、コンテンツ記録手段254によってネットワーク500を介してディスクDに記録する。一方、第2関数化手段255では第1DI読み取り手段251で読み取られた固有情報DIを第1関数化手段252とは異なる関数F'によって関数化してF'(DI)とし、DI記録手段256においてネットワーク500

を介してディスクDに記録する。

【0051】次に、ユーザーが情報再生手段300において情報記録媒体Dを再生する場合について説明する。まず、情報記録手段200で正規に記録されたオリジナルのディスクDを再生する場合には、まずディスクDからDI読み取り手段301によってディスクDの固有情報DIを読み取り、この固有情報DIをDI関数化手段302で関数化してF(DI)とする。ここで、オリジナルのディスクDを再生する場合には、差分読み取り手段308では差分を読み取る必要はなく、合成手段309でも合成することはない。そこで、コンテンツ復号化手段307ではコンテンツ読み取り手段306によって読み取られた暗号化されたコンテンツE(CT)を復号化してコンテンツCTとし、出力手段400に送り、出力することになる。

【0052】次に、コピーされたディスクD'を再生する場合について説明する。この場合には、DI読み取り手段301によって読み取られた固有情報DI'がディスクDの固有情報DIと異なるので、このままではディスクD'を再生することができない。そこで、情報記録手段200の第2DI読み取り手段257によって関数化された固有情報F'(DI)を読み取り、DI復号化手段258で逆関数 F'^{-1} をかけることによって固有情報DIを得る。このように、F'(DI)をあらかじめオリジナルのディスクDに記録しておき、逆関数 F'^{-1} を保存しておくことによって、オリジナルのディスクDの固有情報DIを復号化して得ることができる。また、逆関数 F'^{-1} をコンテンツを供給する側のみが知るようにしておくことによって、不正にコピーされることを防止することもできる。

【0053】そして、このようにして得た固有情報DIを第1関数化手段252によって関数化し、F(DI)を得る。また、第1DI読み取り手段251ではコピーディスクD'の固有情報DI'を読み取り、第1関数化手段252で関数化してF(DI')を得る。

【0054】ここで、差分手段259では、関数化された固有情報F(DI)、F(DI')の差分 $F(DI)-F(DI')$ を生成し、差分記録手段260によってネットワーク500を介してディスクD'に記録する。この際、ディスクD'のF'(DI)が記録されている部分に重ね書きをしても、別のエリアに記録してF'(DI)を残しておいてもよい。また、この差分 $F(DI)-F(DI')$ をディスクD'に記録する際にコンテンツを供給する側では料金を徴収すればよい。

【0055】そして、情報再生手段300では差分読み取り手段308によって差分 $F(DI)-F(DI')$ をディスクD'から読み取り、この差分 $F(DI)-F(DI')$ とDI関数化手段302で関数化されたF(DI')とを合成手段309で合成してF(DI)を得る。このF(DI)によってコンテンツ復号化手段307で

は、コンテンツ読み取り手段 306 で読み取られた暗号化されたコンテンツ E (CT) を復号化してコンテンツ C T とし、出力手段 400 に送り、出力することになる。

【0056】尚、本実施形態では、ネットワーク 500 を介して情報記録媒体 D への記録、読み取りを実行しているが、ネットワーク 500 を介さずに情報記録手段 200 から情報記録媒体 D に直接記録等してもよい。

【0057】このように、第 2 の実施形態の情報保護装置によれば、あらかじめ F' (D I) をオリジナルのディスク D に記録しておき、逆関数 F' ⁻¹ を D I 復号化手段 258 に保存しておくことによって、オリジナルのディスク D の固有情報 D I を復号化して知ることができる。さらに、このオリジナルディスク D の固有情報 D I とコピーディスク D' の固有情報 D I' とから差分を生成してコピーディスク D' に記録することによって、情報再生手段 300 では、この差分とコピーディスク D' の関数化された固有情報 F (D I') とを合成して F (D I) を得ることができるので、暗号化されたコンテンツを復号化することができる。

【0058】また、コンテンツを供給する側としては、差分 F (D I) - F (D I') をディスク D' に記録する際に、料金を徴収すればよいので、利益を確保することができるとともに、ディスクコピーによってコンテンツの使用を許可できるのでコンテンツの流通性をよくすることができる。

【0059】さらに、逆関数 F' ⁻¹ をコンテンツを供給する側のみが知るようにしておくことによって、不正にコピーされることを防止することもできる。

【0060】次に、情報記録媒体への固有情報の記録について説明する。

【0061】本発明の情報保護方法において、まず不正コピーを防止するためには情報記録媒体に記録されている固有情報 D I が容易に改竄できない方法で記録されていなければならない。

【0062】同心円状あるいはスパイラル状に情報を記録する任意の追記型あるいは書換型の一般的な情報記録媒体（以下、ディスク媒体と証する）は、図 3 に示すように、一般利用者は記録することができない領域、すなわち B C A（バースト・カッティング・エリア）3 やリードインエリア 2 などとユーザーが記録できる領域、データエリア 1 などで構成されることが多い。このようなディスク媒体において、固有情報 D I（番号・記号・文字・データなど任意の形態でよい）を特定のエリアに記録するか、あるいは例えばディスク媒体生産時に記録しておく方式を用いることによって、ディスク媒体それぞれを識別することが可能となる。

【0063】ここで、固有情報 D I とは、各ディスク媒体をそれぞれ識別可能な唯一、あるいは他のディスク媒体の固有情報 D I とは容易に一致しない情報のことである。また、特定のエリアとは、例えば図 3 の B C A（バ

ースト・カッティング・エリア）3、リードインエリア 2、データエリア 1 などに記録することができるが、これらの場所に限らず任意の場所に記録することができるものである。

【0064】このような固有情報 D I は、ユーザーが記録できない、あるいは記録されているものを改竄できない方法で記録することが必要であり、例えばディスク上に機械的な凹凸であらかじめ記録しておいたり、強いレーザー光のオンオフなどでディスクの微小領域の組成や破壊による反射率の変化で記録したり、あらかじめ機械的に記録されている信号の一部を破壊するなどの方法で記録することができる。

【0065】

【発明の効果】以上説明したように、本発明の情報保護方法及び情報を保護するための情報記録媒体によれば、第 1 の実施形態では各ディスクに特有の固有情報だけでなく、各コンテンツに特有の識別情報 C I とを利用することによって、不正コピーを防止できるとともに正規の手続きをした者は容易にディスクのコピーができるようになった。

【0066】第 2 の実施形態では、別の関数で関数化した固有情報 F' (D I) をオリジナルのディスク D に記録しておき、逆関数 F' ⁻¹ を D I 復号化手段 258 に保存しておくことによって、オリジナルのディスク D の固有情報 D I を復号化して知ることができ、さらに差分を利用することによって、不正コピーを防止できるとともに正規の手続きをした者は容易にディスクのコピーができるようになった。

【0067】また、コンテンツを供給する側としては、正規の手続きをした者から料金を徴収することによって、利益を確保することができることになった。

【図面の簡単な説明】

【図 1】本発明に係る情報保護方法を実現する装置の第 1 の実施形態の構成を示すブロック図である。

【図 2】本発明に係る情報保護方法を実現する装置の第 2 の実施形態の構成を示すブロック図である。

【図 3】情報記録媒体であるディスクの構成を示す図である。

【図 4】従来の情報保護装置の構成を示すブロック図である。

【図 5】従来の情報保護装置の構成を示すブロック図である。

【図 6】図 4 に示す従来の情報保護装置において、ネットワークを介する場合における構成を示すブロック図である。

【図 7】図 5 に示す従来の情報保護装置において、ネットワークを介する場合における構成を示すブロック図である。

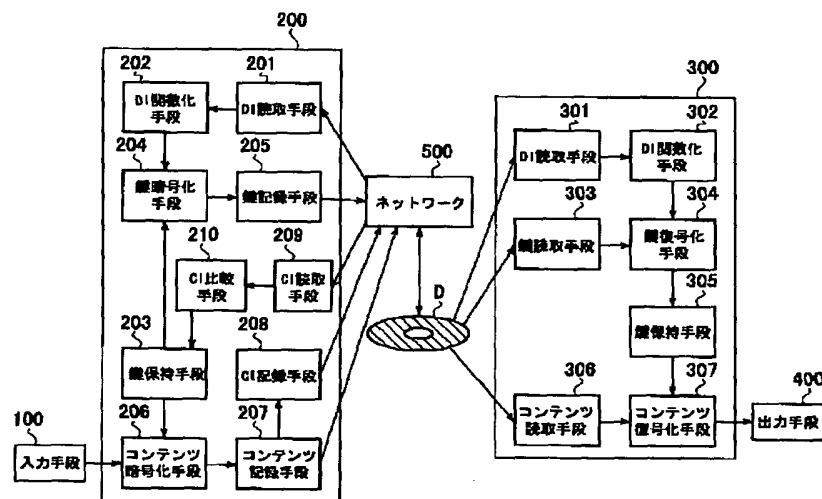
【符号の説明】

1 データエリア

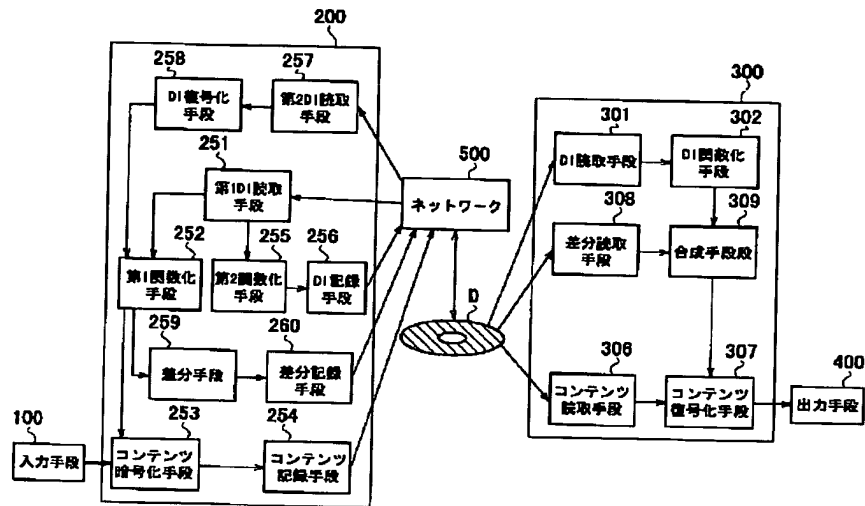
2 リードインエリア
 3 パースト・カッティング・エリア
 10、100 入力手段
 20、200 情報記録手段
 21、31 DI読み取り手段
 22、32 DI関数化手段
 23 コンテンツ暗号化手段
 24 コンテンツ記録手段
 25 鍵保持手段
 26 鍵暗号化手段
 27 鍵記録手段
 30、300 情報再生手段
 33 コンテンツ読み取り手段
 34 コンテンツ復号化手段
 35 鍵読み取り手段
 36 鍵復号化手段
 37 鍵保持手段
 40、400 出力手段
 50、500 ネットワーク
 201、301 DI読み取り手段
 202、302 DI関数化手段
 203 鍵保持手段
 204 鍵暗号化手段

205 鍵記録手段
 206、253 コンテンツ暗号化手段
 207、254 コンテンツ記録手段
 208 CI記録手段
 209 CI読み取り手段
 210 CI比較手段
 251 第1DI読み取り手段
 252 第1関数化手段
 255 第2関数化手段
 256 DI記録手段
 257 第2DI読み取り手段
 258 DI復号化手段
 259 差分手段
 260 差分記録手段
 303 鍵読み取り手段
 304 鍵復号化手段
 305 鍵保持手段
 306 コンテンツ読み取り手段
 307 コンテンツ復号化手段
 308 差分読み取り手段
 309 合成手段
 D 情報記録媒体

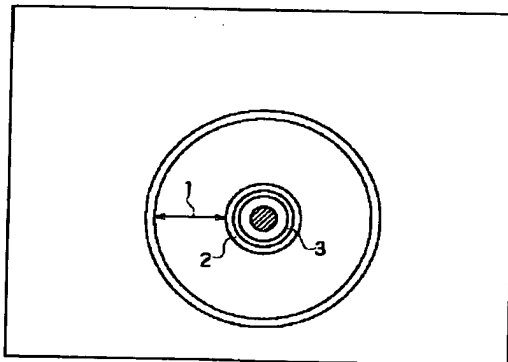
【図1】



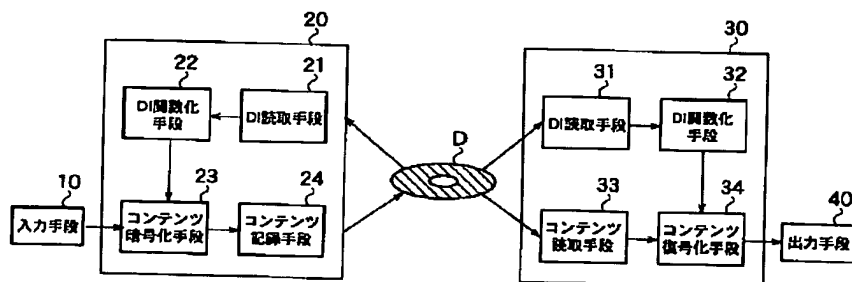
【図 2】



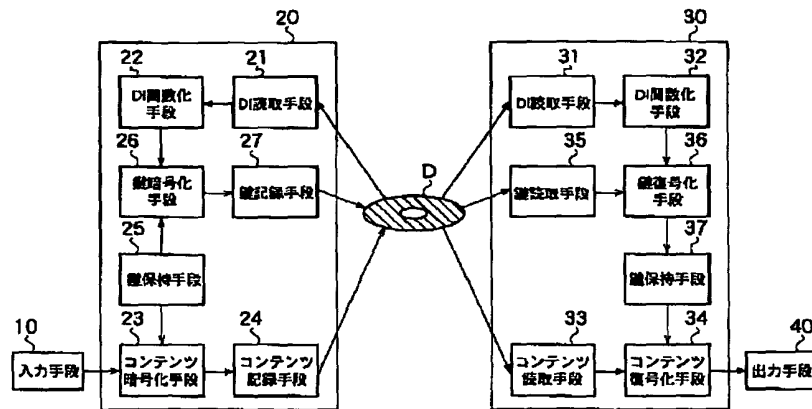
【図 3】



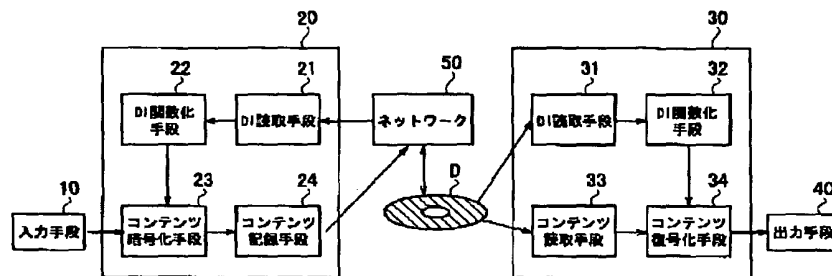
【図 4】



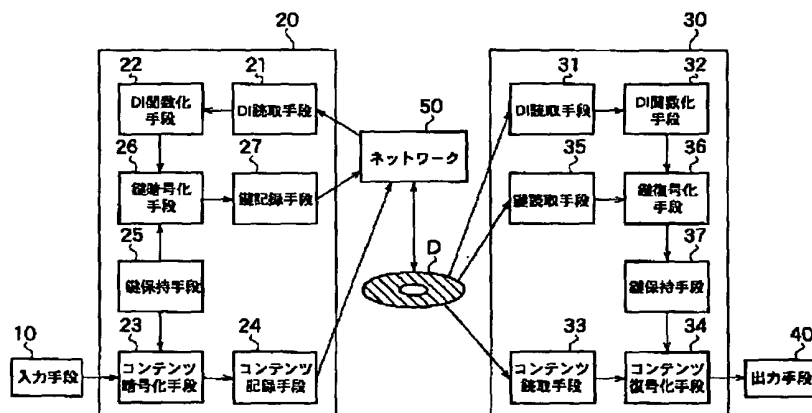
【図5】



【図6】



【図7】



【手続補正書】

【提出日】平成11年7月27日（1999. 7. 27）

【手続補正1】

【補正対象書類名】図面

【補正対象項目名】図4

【補正方法】変更

【補正内容】

【図4】

